UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,662	03/31/2004	Naoki Naruse	9683/183	5965

79510 7590 07/21/2008
NTT Mobile Communications Network I/BHGL
P.O. Box 10395
Chicago, IL 60610

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
07/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/814,662	NARUSE ET AL.	
	Examiner	Art Unit	
	PETER POLTORAK	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 7-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 7-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/21/08 has been entered.

Response to Arguments

2. In light of applicant's amendments and arguments the objection to claim 18 is withdrawn.
3. As per claim 1 and 18, it appears that applicant challenges the examiner's interpretation of a third file summarizing that Stalling does not teach three files. In order to support the allegation applicant discloses the Stalling's Fig. 8.5 (e) used in the rejection and summarizes Stalling's teaching that "addition of S..." *("common secret value")* "...prior to the hash step does not result in a third file as presently claimed".
4. The examiner was not able to find the recitation in claims 1 and 18 (or in claims 1, 7, 11, 18-19 and 23, additionally cited in regard to the argument) stating that a third file is a result of addition of common secret value prior to the hash step. Thus, the above arguments are not persuasive.
5. *Applicant disagrees that "the second file (as properly interpreted) is 'input to the one-way function to generate the second file calculated value'" and states that "instead,*

as properly interpreted, the message M is the first file so that first file (instead of the second file) is input to the one-way function, similar to the teaching of the Angelo reference…".

The examiner points out that the claim language states a part of the second file (and clearly, as shown in Fig. 8.5(e), the first file (M), which is a part of the second file indeed is used in generation of the second file calculated value) and not the entire second file is input to the one-way function.

6. *Additionally, applicant argues that checking whether the received hash file is valid (i.e. whether is the same as expected hash file that is derived from the same message) is validation of the message (first file) and no the hash (second file).*

The examiner points out that comparing hash that is expected to be derived from a message against a newly calculated hash calculated from the same message reads on a process of hash validation.

7. At pages 11-13, applicant argues Angelo and Feghhi references.

As per applicant's question "where is the motivation that 'an ordinary artisan would readily recognize a security weakness of Angelo invention…'" the examiner points out that the security weakness of Angelo, that discloses a hash and a public key to validate hash being used together without the proof of authenticity of the public key is the motivation.

In order to prevent confusion, in this Office Action the examiner offers alternative language, although the same rejection is maintained, to more clearly articulate Angelo in view of Feghhis' combination.

8. *As per applicant's suggestions that Feghhi would not address the security weaknesses of Angelo. In particular, applicant suggests that "the certificate can be used to verify that a public key belongs to a particular individual. For example 'Alice' may have a public key for various transactions" and completes with the statement that "the digital certificate cannot be used to verify that the public key associated with it is for 'Alice'" (see last paragraph pg. 11 and the first paragraph of page 12).*

The examiner is not sure whether applicant statement is understood, since it appears that the presented logic comprises contradiction:

"the certificate can be used to verify that a public key belongs to a particular individual" for example Alice,

then

"the digital certificate cannot be used to verify that the public key associate with it is for 'Alice'".

As clearly disclosed by Fegghi, certificate certificates authenticity of the public key that corresponds to a specific user and this authenticity is certified by Certification Authoritie,s which are trusted organization (see Fegghi, pg. 61-63, 63 in particular, pg. 79-80 and Fig. 3-2 on pg. 67).

Additionally, applicant questions the relevance of Fegghi's teaching to Angelo's invention in light of the claim language.

The examiner points out that Angelo discloses a first file comprising the application data and a second file comprising application validity data and running the software

if computed signatures match. The second file comprises a digital signature (signed hash) with associated public key (for checking the signature).

What's missing in Angelo's teaching is a third file comprising second file validity data calculated with a one-way function and used to verify the second file.

Fegghi discloses certificate that includes a Certificate Authority's Digital Signature (signature is calculated with a one-way function) and the authenticity of the public key. (Recall that in Angelo's disclosure a public key is used to verify the second file but the authenticity of the public key is not offered) Thus, Fegghi's disclosed certificate reads on a third file comprising second file validity data calculated with a one-way function and used to verify the second file and the motivation to combine is disclosed in the previous Office Action (see pg. 6-7) and in this Office Action, below. (For applicant's convenience the motivation is presented in the alternative language).

9. **Summarizing:**

It appears that applicant misunderstood the Angelo and Feghhi's references and their relevance to the claim language. Although the previous rejection is maintained, the examiner offers the alternative language in order to articulate the previously cited rejection. Note, that the previous rejection still applies, since it is the same rejection but expressed using different language, for applicant convenience.

Also, it appears that applicant intends a special interpretation of some of the terms used in the claim language (e.g. a file (the second file) cannot comprise other files (the first and the third files, for example)). Although, files that are part of other files

are old and well known in the art of computing (for example XML files with various incorporated files such as text, music, video components, and email text with attachments; both XML and email can also include a digital signature, etc.) the examiner agrees that explicit claim language (or definition in the specification) prohibiting the first file to comprise the first and the third file would overcome Stallings in view of Angelo rejection. However, the original specification would have to support such interpretation and/or amended language.

10. Claims 1 and 7-29 have been examined.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

11. Claims 1, 7-11, 15, 17-23, 27, 29 remain rejected under 35 U.S.C. 103(a) as obvious over Stallings (William Stallings, "Cryptography and network security", 2th edition, 1998, ISBN: 0138690170) in view of Angelo (USPUB 2003/0061487).

Stallings discloses **a first file (message M)** and **a third file** (**hash** of the first file: H(MIIS) that is put **together in a second file**, illustrated as a two color rectangle in Fig. 8.5 (e), for example.

As per claims 1, 7, 11, 18-19, 23 the examiner interprets the first file to read on application data, bits value in the second file to read on the application validity data and bits value in the third file as a second file validity data.

As seen in Fig. 8.5 (e) a communication device (Destination) receives the first, second and third values. At least a part of the second file (the first file: M of the first file comprising M and H(MIIS)) is input at the Destination to the one-way function to generate the second file calculated value (H). The examiner interprets the result of the calculation as a second file calculated value. As clearly disclosed in Fig. 8.5 (e) the second file calculated value is compared with the second file validity data in the third file. Since a one-way function uniquely identifies data, the comparison inherently enables determining whether the second file is valid based on the second file calculated value with the second file validity data in the third file.

An ordinary artisan would readily recognize the application validity data (the second file) inherently verifies whether the application data (M) in the second file is valid, and, since hash (H) is derived from M a positive comparison ensure that the second file is valid. (Putting in plain language if a hash appended to and derived from a message equal to a copy of hash newly generated the message, the message and the original hash are verified to be valid.)

In other way to look at it is to say that, if the second file (M and H(MIIS), that is both M and H are valid) it verifies that the application data in the first file (M) is valid and as it was established above, this validity would have to been established using the application validity data in the second file (H).

Stallings is silent in regard to executing the application data on the communication device if above discussed validities are established, or putting simply, when a message and the associated hash are valid.

Angelo (USPUB 2003/0061487) discloses executing application data (which is a program) when it is determine that a message and the associated hash are valid (Angelo, [22]).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to execute the application data if the message and the hash are valid. One of ordinary skill in the art would have been motivated to perform such a modification in order to increased system's security.

12. Claims 8-10, 15, 20-22 and 27 recite the same inherent features of the discussed above message authentication using a message hash, and as per claim 22, an ordinary artisan would readily recognize that in other to derive the same hash of the message the hash function must be the same (see text associate with Fig. 8.5 (e) on pg. 247.

13. As per the limitation of claims 17 and 29, the examiner points out that in the situations where a file comprises more than one file, additional data must be included in order to enable a proper interpretation of values, that is in order to identify which values belong to which data, or in other words, how to read and interpret the received data. This additional data identifies location of particular parts of the data (note that the location can be identified either explicitly, the end of data or the beginning of new data, or not explicitly, a type of protocol used which distinguishes which anticipate a particular location for a particular data). The examiner interprets this additional data to be a part of the second file.

14. Claims 1, 7-13, 15, 18-25 and 27 remain rejected under 35 U.S.C. 103(a) as obvious over Angelo (USPUB 2003/0061487) in view of Feghhi (Jalal Feghhi, Jalil Feghhi, Peter Williams, "Digital Certificates Applied Internet Security, 1999, ISBN: 0201309807).

The examiner refers to one-way function as hash or hash function, which is consistent with the practice in the art of computer security.

15. Angelo discloses executing application data (which is a program) when it is determine that a message and the associated hash, or a digital signature (to be more exact) are valid (Angelo, [22]).

In paragraphs 22-23 Angelo discloses as follows:

> "In accordance with the preferred embodiment of the invention, however, the operating system preferably performs the following security feature, or otherwise causes the following security feature to be performed. The workstation computer on which the application is to run preferably computes a hash of the copy of the object code to be executed thereon. The hash function used by the computer preferably is the same hash function that was used to create hash H1 stored in the security database 110. The workstation computer also retrieves the previously computed, signed hash H1 from the security database corresponding to the program to be run. The computer decrypts the signed hash using a public key that corresponds to the private key used to encrypt the hash in the first place.
>
> The computer then compares the two hashes--the newly computed hash of the particular copy of the object code to be executed and the previously computed hash of presumably the same object code. If the object code has been modified in any way, the newly computed hash will differ from the previously

computed hash. Accordingly, the computer 104-108 attempts to authenticate its copy of the object code to be executed by comparing the two hashes. If they match, then computer determines that the object code is authentic, and then proceeds with running the software. "

A file comprising the application disclosed by Angelo reads on a first file comprising the application data. A file storing a digital signature (signed hash) with associated public key (for checking the signature) reads on a second file comprising application validity data and running the software if computed signatures match as taught by Angelo clearly shows that the application validity data is used to verify validity of the application data in the first file and that the application data on the communication device is executed if the application data is verified.

16. Angelo does not disclose a third file comprising second file validity data calculated with a one-way function and used to verify the second file.

Feghhi discloses a third file (a certificate, Fegghi, e.g. Fig. 3-2) that includes application validity data calculated with a one-way function and used to verify the second file.

Certification Authority's Digital Signature. The certificate disclosed by Fegghi uses a public key to generate signature and signature is generated using hash (one-way function) of the data (that as seen in Fig. 3-2, includes the public key), the process of verifying the signature, that inherently includes comparing the original value (the second file validity data in the third file) with the second file calculated value (that is a value derived by hashing (inputting to one-way function) at least a part of the second file (the public key).

Hashing data and then signing the hash (that is, encrypting it with a key) as disclosed by Angelo enables to validate the data. Note that by virtue of public/private key cryptography, as long as the corresponding key (whether it is original or substituted malicious) is used to validate the (original or substituted malicious, accordingly) data, the validation is positive.

Consequently, lack of verification of the source data (is it an authentic/original data?) is main flaw of Angelo's teaching and Fegghi's teaching discussed above ensures authenticity of data (digital certificates are issued by Certification Authorities which are trusted organization (e.g. Fegghi, pg. 79-80) and verify authenticity of the keys that sign data). Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to provide a third file comprising application validity data for the predictable result of ensuring authenticity of data (see KSR ruling). *(See additional discussion regarding Angelo in view of Fegghi's combination in Response to Arguments section above, in particular the examiner addressing applicant questioning the relevance of Fegghi's teaching.)*

17. Verifying the second file based on comparing the second file calculated value with the second file validity data in the third file before executing the application data would have being implicit. As discussed before, verifying the second file based on comparing the second file calculated value ensures that the authentic data is generated by a certified subject/entity.

18. Claims 14, 16, 26 and 28 remain rejected under 35 U.S.C. 103(a) as obvious over Angelo (USPUB 2003/0061487) in view of Feghhi (Jalal Feghhi, Jalil Feghhi, Peter Williams, "Digital Certificates Applied Internet Security, 1999, ISBN: 0201309807) in view of Fukumoto(USPUB 2002/0073072).

As discussed above, operations on the received second and third files determines validity of the second file, the third file (digital certificate) disclosed by Fegghi is provided by Certificate Authorities.

19. Angelo in view of Fegghi does not disclose that the second file is received from a content provider server and does not disclose that the receiver receives the first file only after determining validity of the second file.

In analogues art, Fukumoto discloses a receiver (terminal 10) using a certificate to receive application data (program P) from a content provider server (server 30). Fukumoto discloses that a first file is received after determining validity of a second file (Fukumoto, [58]). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure Angelo in view of Fegghi's system to receive the first file only after determining validity of the second file. One of ordinary skill in the art would have been motivated to perform such a modification given the benefit of improved security. Note that determining validity of the second file in addition to operating on the second file included operating on the third file.

Conclusion

All claims are drawn to the same invention claimed in the earlier application and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the earlier application. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action in this case. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Peter Poltorak/

Examiner, Art Unit 2134

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134